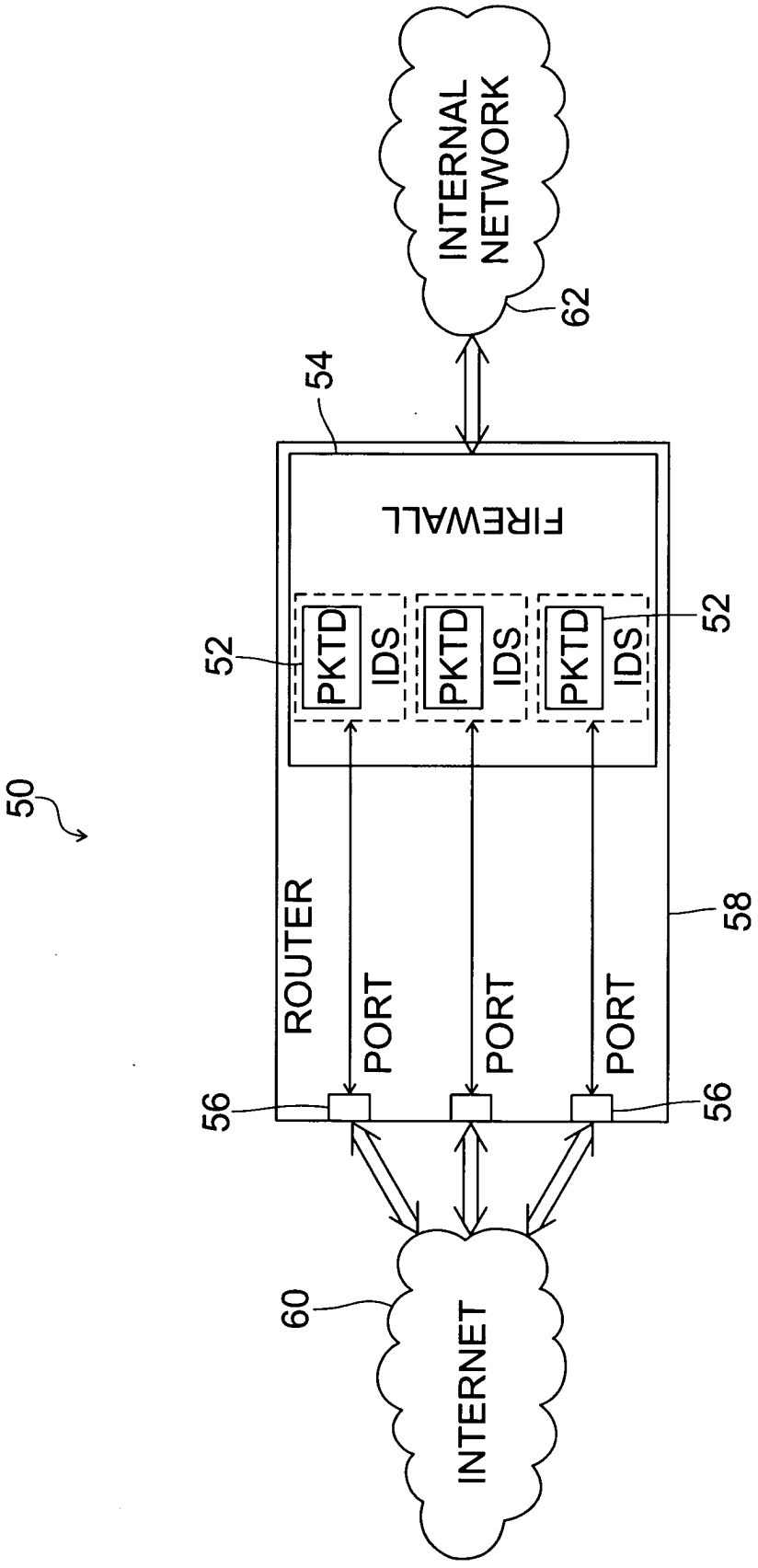
INTERNAL NETWORK
62
54
FIREWALL
PKTD
IDS
PKTD
IDS
PKTD
IDS
52
52
50
ROUTER
PORT
PORT
PORT
58
56
56
60
INTERNET

Fig. 1

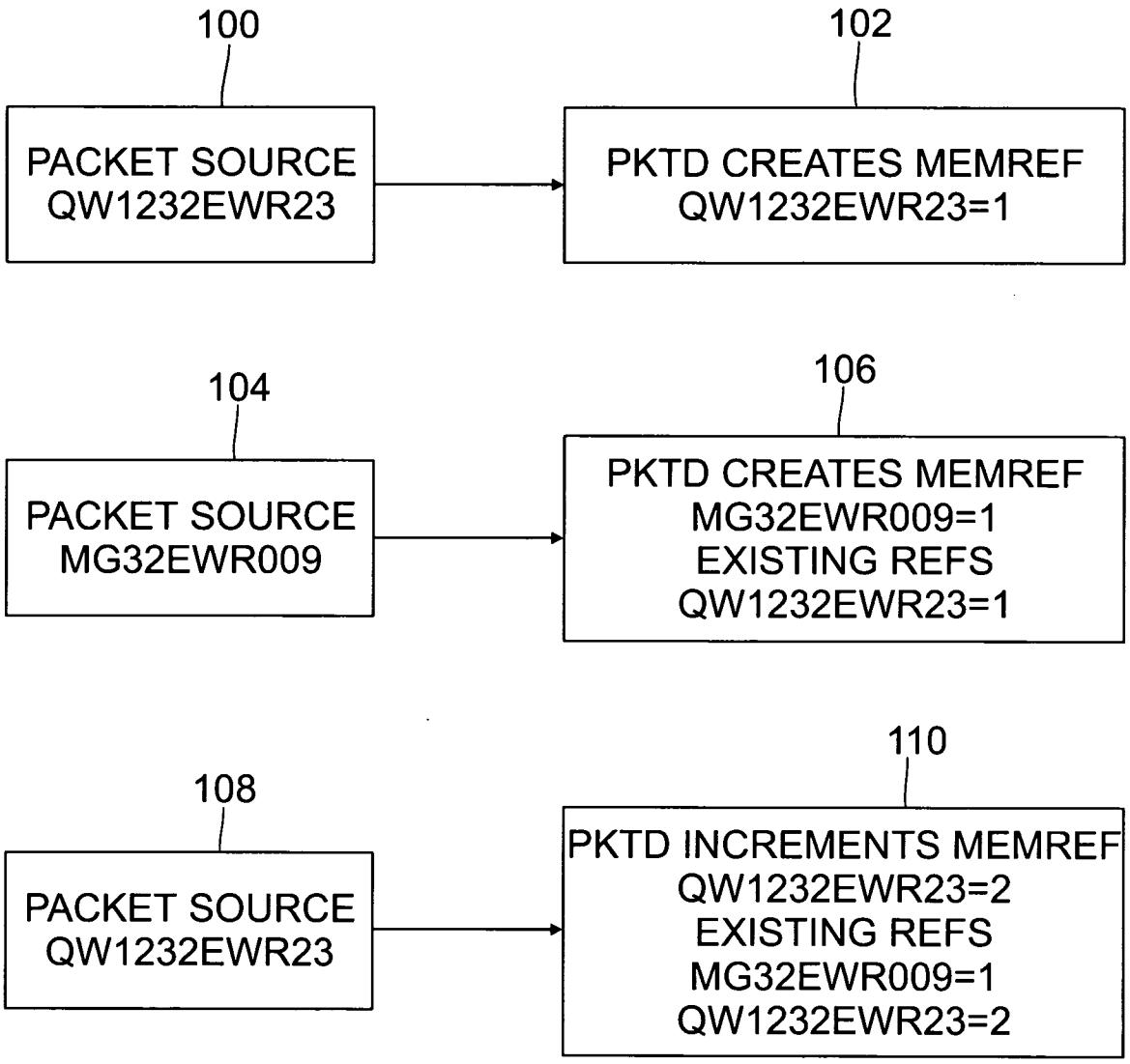
100
PACKET SOURCE
QW1232EWR23
102
PKTD CREATES MEMREF
QW1232EWR23=1
104
PACKET SOURCE
MG32EWR009
106
PKTD CREATES MEMREF
MG32EWR009=1
EXISTING REFS
QW1232EWR23=1
108
PACKET SOURCE
QW1232EWR23
110
PKTD INCREMENTS MEMREF
QW1232EWR23=2
EXISTING REFS
MG32EWR009=1
QW1232EWR23=2

Fig. 2

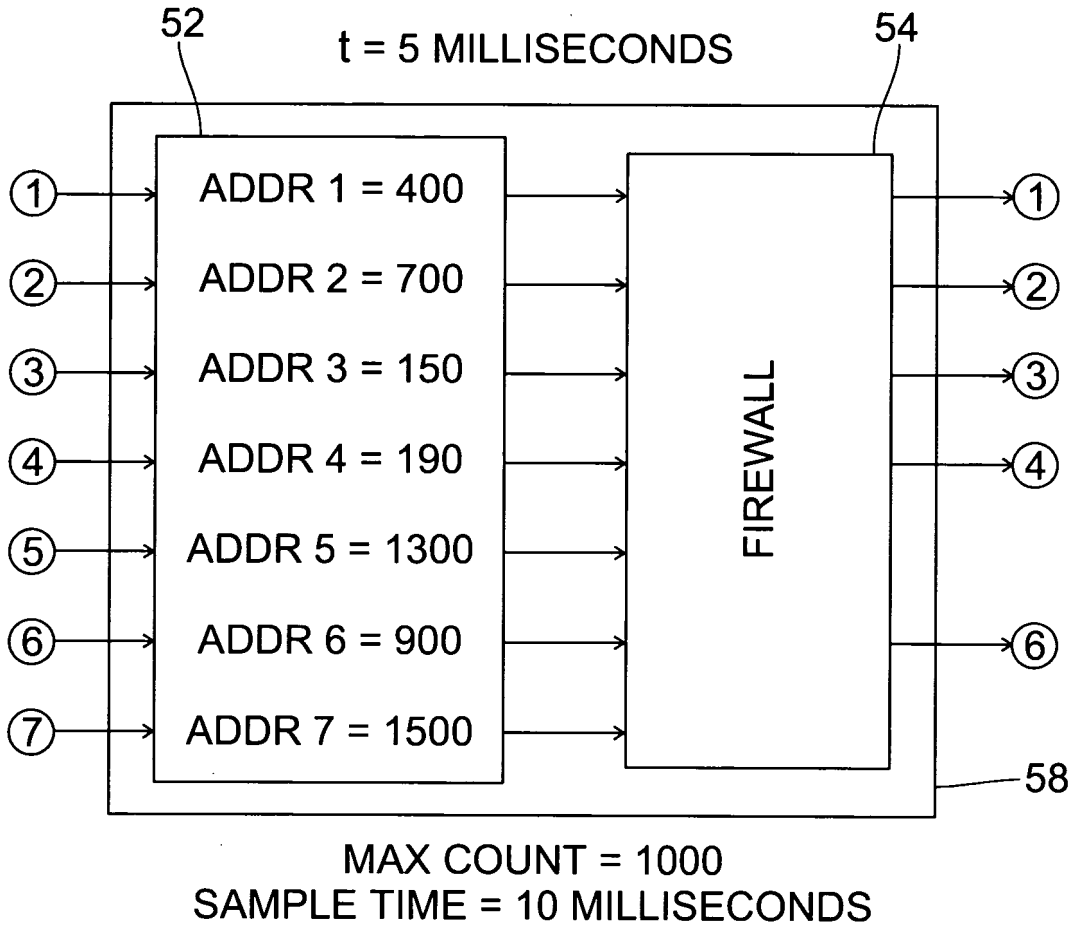
52
t = 5 MILLISECONDS
54
ADDR 1 = 400
ADDR 2 = 700
ADDR 3 = 150
ADDR 4 = 190
ADDR 5 = 1300
ADDR 6 = 900
ADDR 7 = 1500
FIREWALL
1
2
3
4
5
6
7
1
2
3
4
6
58
MAX COUNT = 1000
SAMPLE TIME = 10 MILLISECONDS

Fig. 3

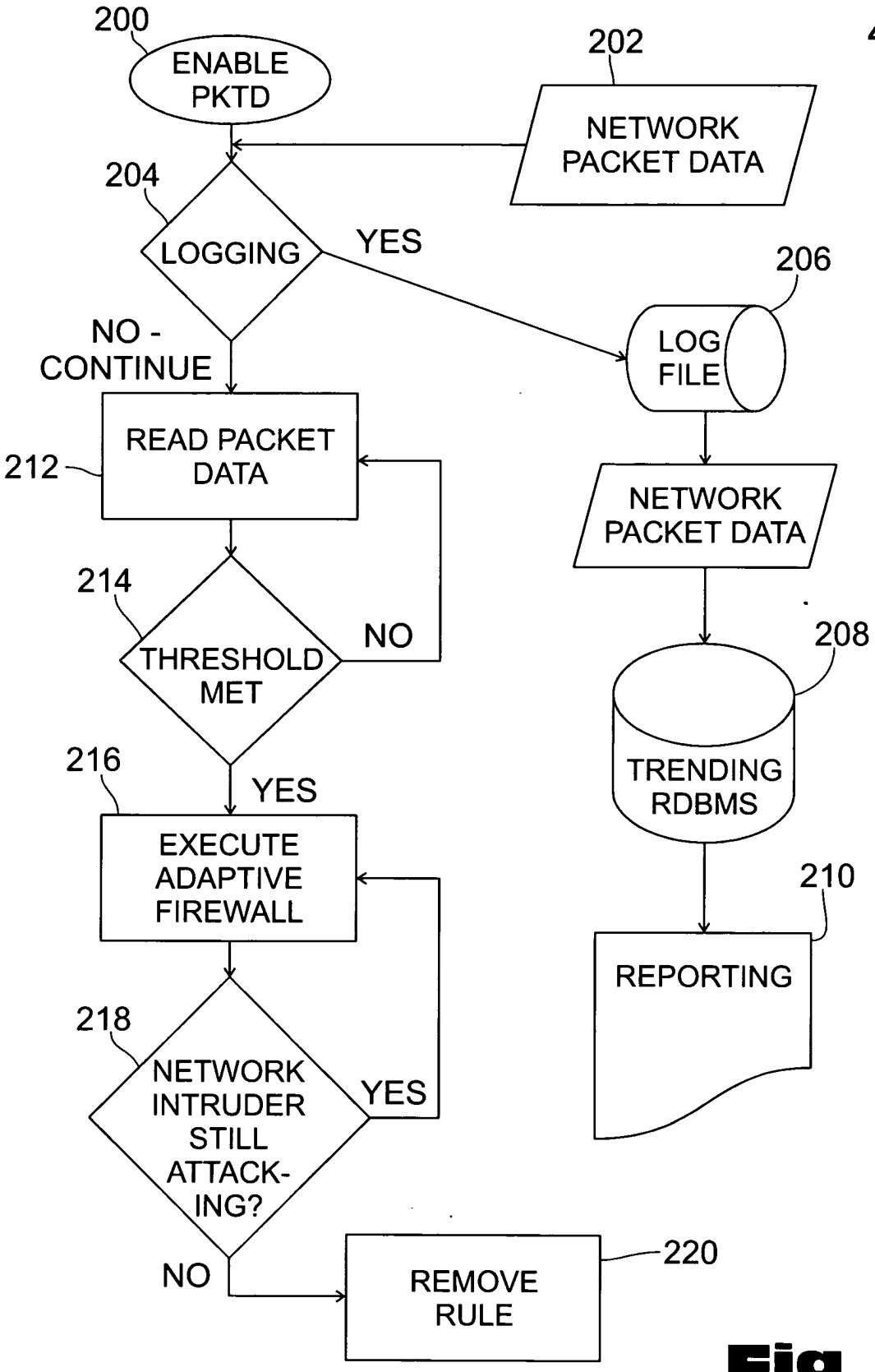
200
ENABLE PKTD
202
NETWORK PACKET DATA
204
LOGGING
YES
206
LOG FILE
NO - CONTINUE
READ PACKET DATA
212
NETWORK PACKET DATA
214
THRESHOLD MET
NO
208
TRENDING RDBMS
216
YES
EXECUTE ADAPTIVE FIREWALL
210
REPORTING
218
NETWORK INTRUDER STILL ATTACK-ING?
YES
NO
220
REMOVE RULE

Fig. 4

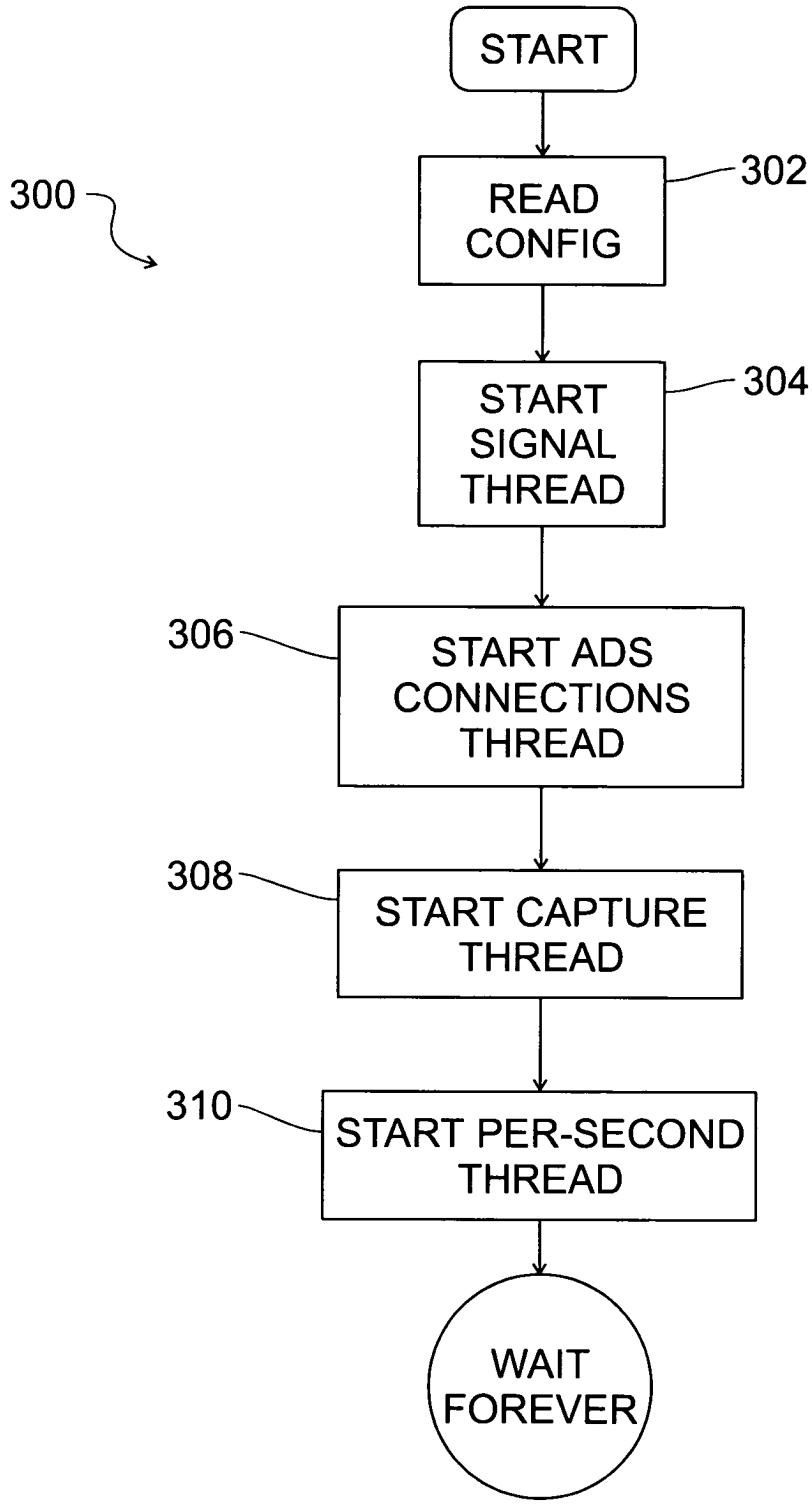
300
START
READ CONFIG
302
START SIGNAL THREAD
304
306
START ADS CONNECTIONS THREAD
308
START CAPTURE THREAD
310
START PER-SECOND THREAD
WAIT FOREVER

Fig. 5

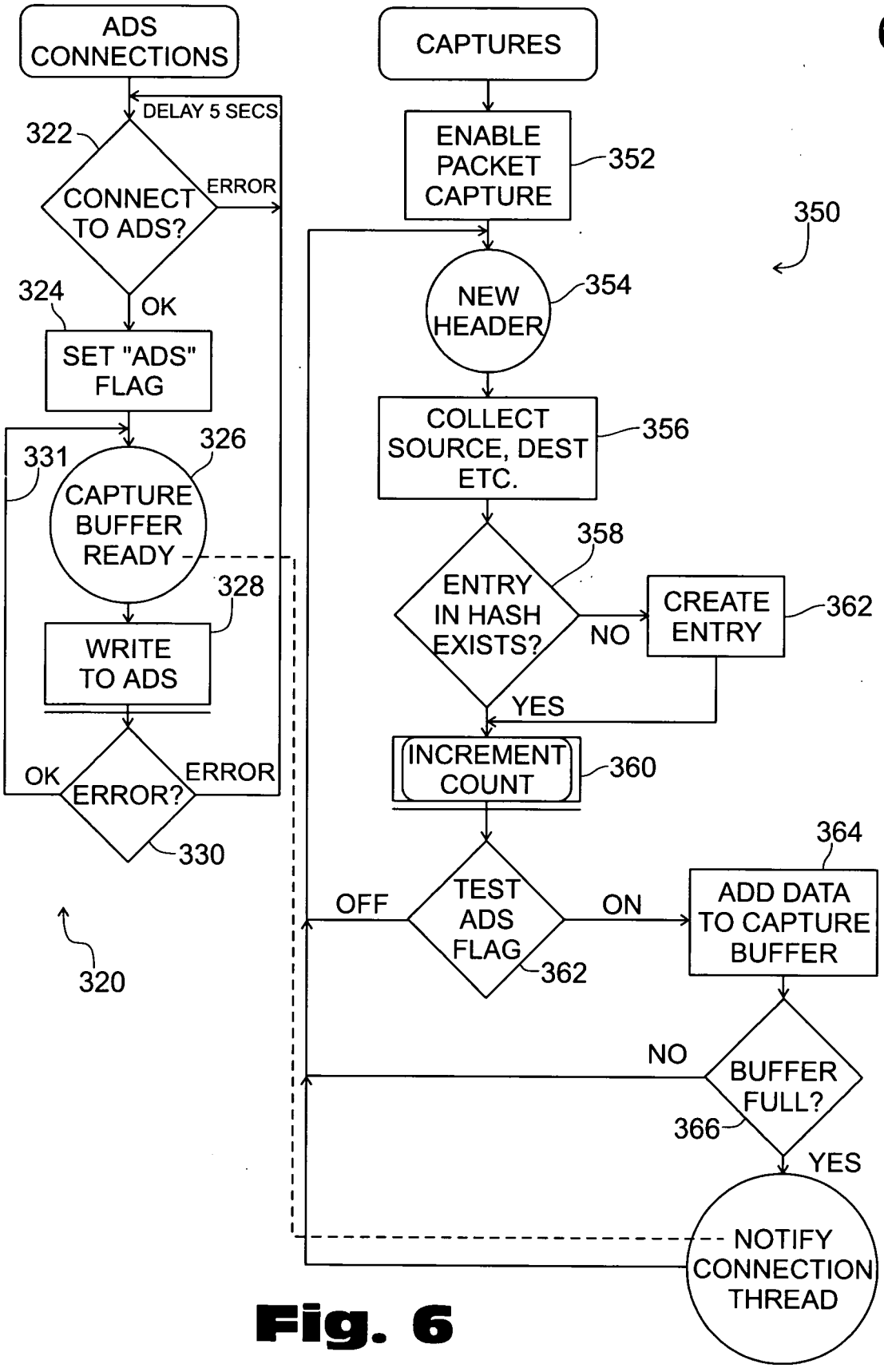
ADS CONNECTIONS
DELAY 5 SECS
322
CONNECT TO ADS?
ERROR
OK
324
SET "ADS" FLAG
326
331
CAPTURE BUFFER READY
328
WRITE TO ADS
OK
ERROR?
ERROR
330
320
CAPTURES
ENABLE PACKET CAPTURE
352
350
NEW HEADER
354
COLLECT SOURCE, DEST ETC.
356
358
ENTRY IN HASH EXISTS?
NO
CREATE ENTRY
362
YES
INCREMENT COUNT
360
364
OFF
TEST ADS FLAG
362
ON
ADD DATA TO CAPTURE BUFFER
NO
BUFFER FULL?
366
YES
NOTIFY CONNECTION THREAD

Fig. 6

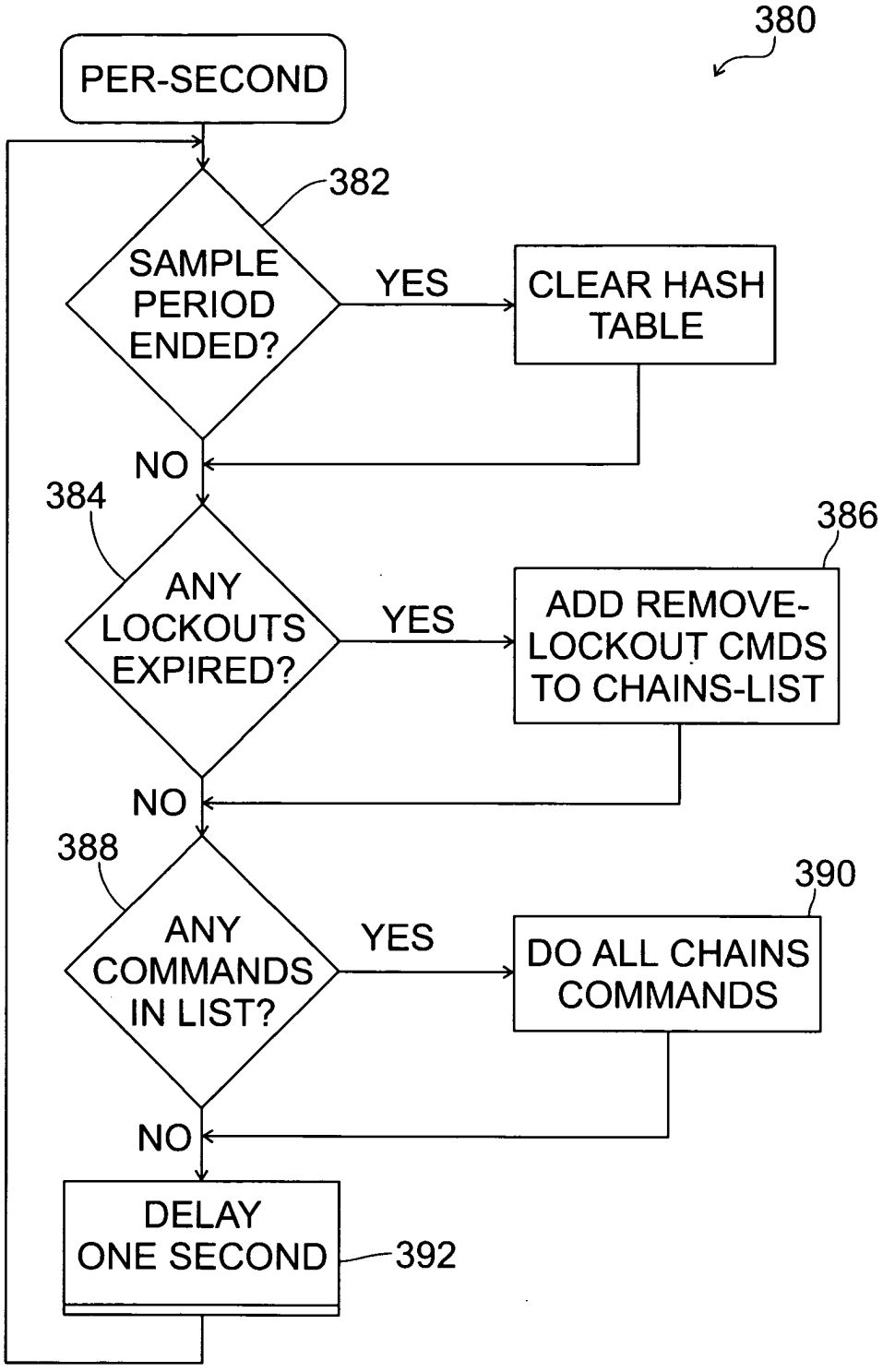
380
PER-SECOND
382
SAMPLE PERIOD ENDED?
YES
CLEAR HASH TABLE
NO
384
386
ANY LOCKOUTS EXPIRED?
YES
ADD REMOVE-LOCKOUT CMDS TO CHAINS-LIST
NO
388
390
ANY COMMANDS IN LIST?
YES
DO ALL CHAINS COMMANDS
NO
DELAY ONE SECOND
392

Fig. 7

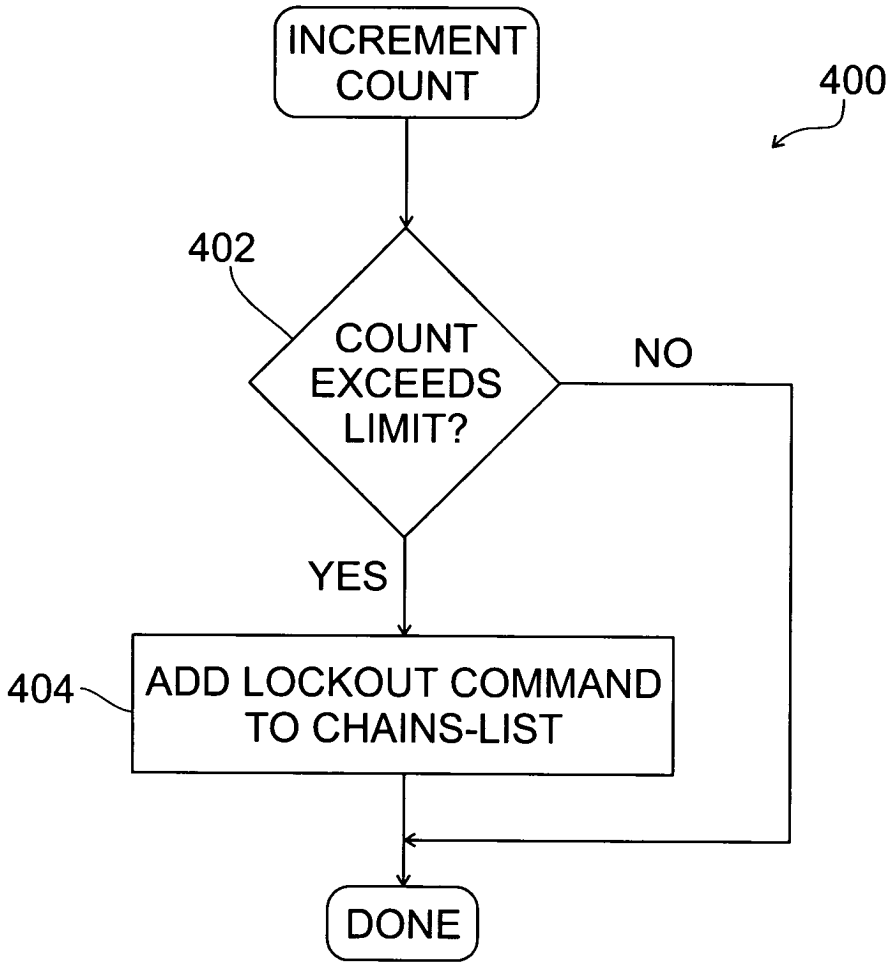
INCREMENT COUNT
400
402
COUNT EXCEEDS LIMIT?
NO
YES
404
ADD LOCKOUT COMMAND TO CHAINS-LIST
DONE

Fig. 8

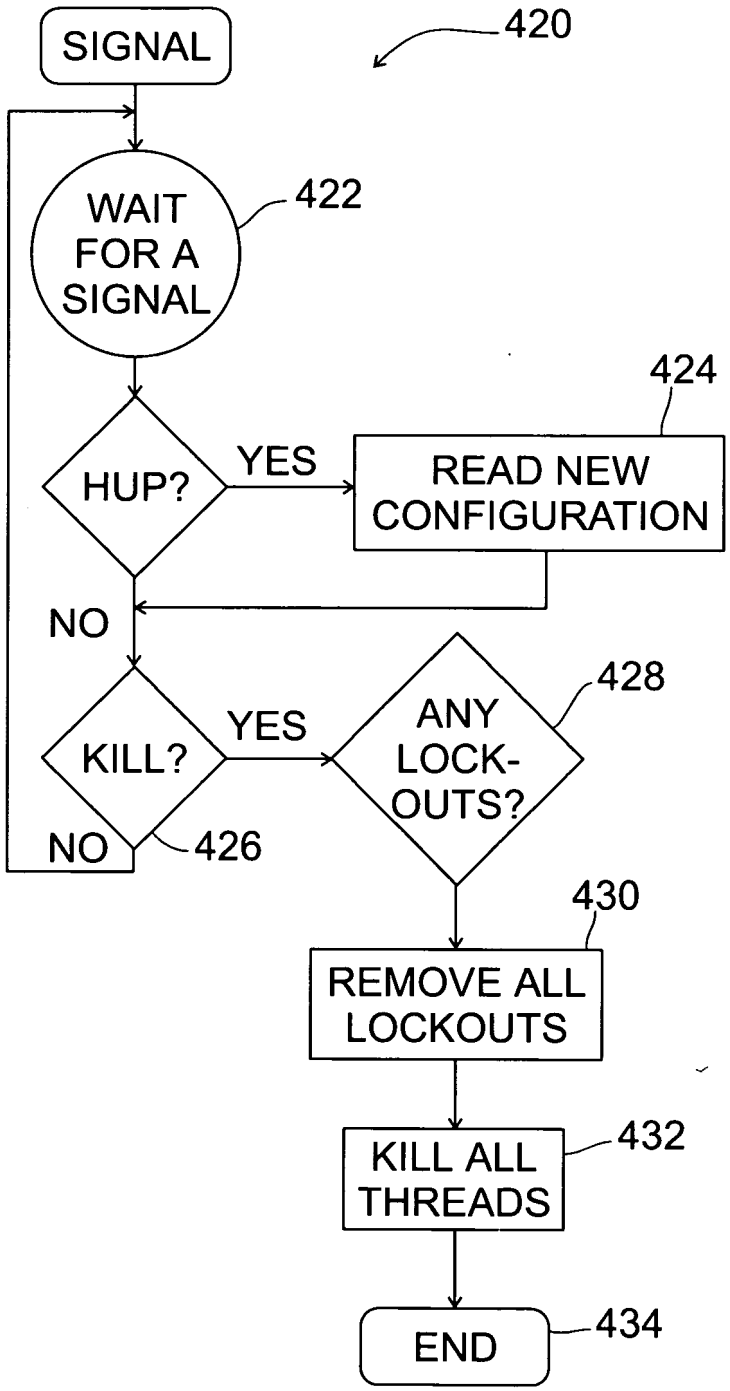
SIGNAL
420
WAIT FOR A SIGNAL
422
HUP?
YES
424
READ NEW CONFIGURATION
NO
KILL?
YES
ANY LOCK-OUTS?
428
NO
426
430
REMOVE ALL LOCKOUTS
KILL ALL THREADS
432
END
434

Fig. 9